

# Exhibit 223

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

SECURITIES AND EXCHANGE COMMISSION,

Plaintiff,

v.

RIPPLE LABS INC., BRADLEY GARLINGHOUSE, and  
CHRISTIAN A. LARSEN,

Defendants.

No. 20-cv-10832 (AT)

**REBUTTAL EXPERT REPORT OF DR. PETER ADRIAENS**

## TABLE OF CONTENTS

|  |           |
|--|-----------|
| <b>I. INTRODUCTION.....</b>  | <b>1</b>  |
| <b>II. DR. [REDACTED] OPINIONS REGARDING WHETHER THE XRP LEDGER IS DECENTRALIZED REST ON A SELECTIVE METHODOLOGY OF HIS OWN CREATION THAT FINDS INSUFFICIENT SUPPORT IN THE PREVAILING LITERATURE.....</b> | <b>3</b>  |
| A. There is no accepted definition of “decentralization” for purposes of evaluating a particular distributed system, like a blockchain.....  | 3         |
| B. There are no accepted criteria to use to determine whether a given system satisfies a given definition of decentralization. ....  | 6         |
| C. There are no accepted metrics to use to quantify whether a given ledger satisfies criteria for decentralization, especially for purposes of comparing Bitcoin, Ethereum and the XRP Ledger. ....        | 11        |
| <b>III. ADDITIONAL RESPONSES TO DR. [REDACTED] REPORT. ....</b>  | <b>27</b> |

## **I. Introduction**

1. I am a Professor of Engineering, Finance and Entrepreneurship, Director of the Center for Smart/Digital Infrastructure Finance, and co-founder of the University of Michigan FinTech Collaboratory. My complete CV and the nature of my retention and compensation in connection with this case were set forth in my expert report of October 4, 2021.

2. I have been provided the expert report of Dr. [REDACTED] (the “Report”) and asked to evaluate the methodology and conclusions set forth in that report.

3. The facts and data I have relied on and considered in forming my opinions are disclosed in the report. Should additional relevant documents or information be made available to me, I may adjust or supplement my opinions as appropriate.

4. As further set forth below, I conclude:

(1) Dr. [REDACTED] principal opinion – that “the XRP Ledger does not satisfy a basic definition of a decentralized system” (Report at 27) – is not the product of a generally accepted methodology for evaluating the decentralization of a distributed ledger. That is because of three facts that the relevant academic literature establishes, but the Report ignores: (i) neither the scientific community nor the blockchain community<sup>1</sup> has reached consensus about the appropriate definition of “decentralization;” (ii) neither community has reached consensus about the appropriate criteria that should be used to determine

---

<sup>1</sup> See Angela Walch, *Deconstructing ‘Decentralization:’ Exploring the Core Claim of Crypto Systems*, in CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 41–42, 47–48, 68 (Chris Brummer ed., 2019) (discussing how “decentralization” is used “in academic works of relevant disciplines, in discussions within the crypto space, in conference names galore, and in countless reports by businesses, governments and international organizations” and yet “in mainstream discourse, it has been rare to see clear explanations of ‘decentralized’ or ‘decentralization’ when they are used”).

whether a given blockchain satisfies any such definition; and (iii) neither community has reached consensus about the appropriate metrics to use to quantify whether a given ledger satisfies such criteria. Given the reasonable disagreement within the literature about the appropriate criteria to define decentralization, and the appropriate metrics to quantify those criteria, Dr. [REDACTED] identification of what he calls “four main aspects of decentralization” (Report at 5) can only be described as novel; it rests on assumptions and choices he has made that are, in the respects discussed below, unsupported by or inconsistent with the prevailing literature and/or lacking in reliability.

(2) Dr. [REDACTED] related opinion that “[t]he XRP Ledger is centralized compared to Bitcoin and even Ethereum” (Report at 24) also is not the product of a generally accepted methodology. That is so, first, because it rests on an unstated assumption – that it is even possible to compare those three blockchains based on uniform criteria – that fails to account for the fundamental differences in their respective consensus mechanisms. That assumption is demonstrably in conflict with the prevailing literature. Moreover, Dr. [REDACTED] application of his stated methodology is unreliable because the metrics by which he purports to quantify whether the Bitcoin, Ethereum, and XRP blockchains are decentralized do not have an agreed-upon system of measurement. Accordingly, even if Dr. [REDACTED] methodology were reliable (and it is not), his application of that methodology to this case is fundamentally flawed in ways independently sufficient to undermine his conclusions.

**II. Dr. [REDACTED] Opinions Regarding Whether the XRP Ledger is Decentralized Rest on a Selective Methodology of His Own Creation That Finds Insufficient Support in the Prevailing Literature.**

**A. There is no accepted definition of “decentralization” for purposes of evaluating a particular distributed system, like a blockchain.**

5. Dr. [REDACTED] report depends on his adoption (Report at 5) of a particular definition of a decentralized system. [REDACTED] draws this definition from a 2017 paper by Troncoso et al., which defines decentralized systems as “a subset of distributed systems where multiple authorities (parties) control different system components and no authority is fully trusted by all.”<sup>2</sup> Dr. [REDACTED] then, in his own words, “refine[s]” this definition by selecting the “four main aspects of decentralization” that comprise his methodology for applying the definition, which then leads him to conclude that “the XRP Ledger does not satisfy the basic definition of a decentralized system.” (Report at 5.) Accordingly, his opinion rests, in the first instance, on the assumption that the Troncoso definition is authoritative.

6. One immediately apparent flaw in Dr. [REDACTED] approach is that he selectively chooses the Troncoso definition of decentralization and treats it as authoritative, when in fact the Troncoso definition is not generally accepted within the literature – indeed, given the nascency of the field, *no* particular definition of a decentralized system has achieved general acceptance within the literature. Even within the peer-reviewed literature, there is disagreement regarding what features of a system must be examined, and how, when evaluating decentralization. The Troncoso paper cited by Dr. [REDACTED] for a purported “basic definition of a decentralized system”

---

<sup>2</sup> Carmela Troncoso et al., *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments*, PROC. PRIV. ENHANCING TECH. (4) 307, 307 (2017).

(Report at 5) itself recognizes that, within the relevant literature, “there does not exist a foundational treatment *or even an established common definition* of decentralization.”<sup>3</sup>

7. While the Troncoso paper was one attempt to craft such a definition, Dr. [REDACTED] report offers no basis to conclude that the Troncoso definition has become an accepted definition within the field. To the contrary, the Sai paper that Dr. [REDACTED] cites (Report at 9–11), which was published in March 2021 (five years after the Troncoso paper), undertakes a “systematic literature review” to “study decentralization in blockchain” and present “the first in-depth analysis of centralization in blockchains.”<sup>4</sup> The Sai paper identifies 89 articles as “relevant blockchain literature”<sup>5</sup> – yet does not cite the Troncoso paper at all. Rather, the Sai paper relies on a definition of decentralization from a paper by Davidson et al., published in 2016, that Dr. [REDACTED] report does not consider. Davidson offers a substantively distinct definition of decentralization from Troncoso, namely that a system is decentralized “where participants can read, write data, and contribute to consensus without authorization.”<sup>6</sup> To give another example, Wu et al., in a 2020 paper, defined decentralization as a system where “no single individual can destroy transactions in the network, and any transaction request requires the consensus of most participants.”<sup>7</sup> This definition again is substantively different from the Troncoso paper and emphasizes participation as opposed to authorization.

---

<sup>3</sup> *Id.*

<sup>4</sup> A.R. Sai et al., *Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review*, 58 INFO. PROCESS & MGMT. 1, 3 (2021).

<sup>5</sup> *Id.* at 3, 32–35.

<sup>6</sup> *Id.* at 4 (citing Davidson et al., *Economics of Blockchain* (Mar. 8, 2016), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2744751](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751)).

<sup>7</sup> Keke Wu et al., *A Coefficient of Variation Method to Measure the Extents of Decentralization for Bitcoin and Ethereum Networks*, 22 INT’L J. NETWORK. SEC. 191, 192 (2020).

8. Moreover, in connection with drafting this report, I have reviewed the sources cited by Dr. [REDACTED] as well as others I identified through my own research. They do not offer an accepted definition of “decentralization” or the factors relevant to determining whether a particular distributed system or blockchain is or is not “decentralized.” In my reading of the peer-reviewed literature, there is currently no generally settled opinion on the definition of decentralization, nor any generally accepted, reliable tools or metrics to compare or quantify different systems.

9. Dr. [REDACTED] report neither acknowledges the ongoing lack of consensus (in both the scientific and professional blockchain communities)<sup>8</sup> on a definition of “decentralization,” nor defends his choice to adopt the Troncoso definition. That is, he never explains why he chose that definition, let alone whether or why it is superior to other proposed definitions in any respect. This approach renders his opinions fundamentally flawed. It is important and necessary, as a baseline starting point for analyzing the issue of decentralization, to acknowledge the lack of consensus among scientific and professional blockchain communities, which continue to wrestle with, debate, and study what “decentralization” means and how to measure it – as even the papers on which Dr. [REDACTED] relies make clear.<sup>9</sup>

---

<sup>8</sup> Walch, *supra* note 1, at 41–42 (providing a descriptive account of the varied and inconsistent uses of the term “decentralized” among the academic, professional, governmental, and international communities, and noting “it has been rare to see clear explanations of ‘decentralized’ or ‘decentralization’ where they are used”); *see id.* at 47 (“No One Knows What Decentralization Means”); *id.* at 39 (noting that, on June 15, 2018, one day after an official of the Securities and Exchange Commission gave a speech discussing decentralization, the Director of the MIT Digital Currency Initiative said on Twitter, “I’m a little worried people from government agencies are throwing around the word ‘decentralization’ like we know what it means and how to evaluate it”).

<sup>9</sup> Those papers set forth a range of metrics for analyzing centralization or decentralization that Dr. [REDACTED] ignores without explanation even as he relies on the literature for other, narrower purposes. I offer no opinion as to the utility of these metrics, since Dr. [REDACTED] does not apply them in his Report, but rather identify them as evidence of the lack of



**B. There are no accepted criteria to use to determine whether a given system satisfies a given definition of decentralization.**

10. Dr. [REDACTED] report, as part of his “refine[ment]” of the Troncoso definition of decentralization, asserts that there are four main criteria by which to evaluate decentralization: (1) Resilience (which Dr. [REDACTED] states should be measured by a metric called the Nakamoto Coefficient), (2) Inclusiveness, (3) In-Protocol Incentives, and (4) Governance (which Dr. [REDACTED] further refines to (a) Public Face and (b) Tokens Allocated at Genesis). (Report at 5.) These criteria form the structure of Dr. [REDACTED] application of the Troncoso definition of decentralization to Bitcoin (Report at 15–17), Ethereum (Report at 18–19), and the XRP Ledger. (Report at 22–24).
11. Dr. [REDACTED] putative refinement of the Troncoso definition compounds his selection of that definition’s flaws, because it, too, rests on an unproven assertion rather than any authoritative source or methodology. To start, Dr. [REDACTED] offers no citation or support for the proposition that these four factors are either necessary or sufficient to determine whether a particular system is decentralized. To the contrary, Dr. [REDACTED] himself recognizes that there are “additional aspects of decentralization” that relate to various aspects of a blockchain system (sometimes grouped into “layers,” to which I return below), but states without explanation or

---

consensus around appropriate metrics to evaluate the basic concept Dr. [REDACTED] Report purports to address. *See, e.g.,* Sarah Azouvi et al., *Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance*, in FIN. CRYPTOGRAPHY AND DATA SEC. 127, 132 (Aviv Zohar ed., 2018) (analyzing “centrality metrics” including Interquartile range, Interquartile mean, Kolmogorov-Smirnov test, Nakamoto index, Satoshi index, and the Sorensen-Dice index); Adem Gencer et al., *Decentralization in Bitcoin and Ethereum Networks*, in FIN. CRYPTOGRAPHY AND DATA SEC. 439, 440 (Aviv Zohar ed., 2018) (presenting “a comprehensive measurement study on decentralization metrics” including “(1) direct measurements of [Bitcoin and Ethereum] from multiple vantage points, (2) a Bitcoin relay network called *Falcon* that we deployed and operated for a year, (3) blockchain histories of Bitcoin and Ethereum”); Sai et al., *supra* note 4, at 12 (summarizing in Table 2 a taxonomy of centralization-related aspects of public blockchains that includes 6 layers and 13 factors within those layers).

citation that his report “opt[s] to focus on decentralization aspects of systems proper.” (Report at 11.) Dr. [REDACTED] offers no explanation or justification for his decision to abandon those “additional aspects,” nor why his methodology and conclusions remain sound despite that decision.

12. A basic methodological step in creating any novel definition in social and informational sciences<sup>10</sup>—which I argue includes key applications of blockchain technology<sup>11</sup>—is to establish that the components of the definition are both *necessary* and *sufficient* to the conclusion.<sup>12</sup> This is because the purpose of definitions is to establish sufficient shared meaning such that a class of entity can be investigated by a scientific community. This does not preclude that a definition may be adjusted in the light of new understandings as they emerge. However, without meeting the necessary-sufficient criteria, a definition will become either overinclusive (if it contains components that are not necessary) or underinclusive (if its components are not sufficient) to reach a relevant conclusion. Yet Dr. [REDACTED] does not attempt to establish that his four selected criteria are necessary or sufficient to define a blockchain as decentralized. To be clear, I do not deny that the four aspects he focuses on are (or, at least, can be) relevant. But others are discussed in the literature, and it appears that Dr. [REDACTED] subjectively chose those four metrics, omitted others, and ignored key insights from the literature in that regard.

---

<sup>10</sup> Blockchain is an emerging technology in the field of computer science, with many of its applications relating to the field of information science, an academic field primarily concerned with analysis, collection, classification, manipulation, storage, retrieval, movement, dissemination, and protection of information.

<sup>11</sup> See Jaideep Ghosh, *The Blockchain: Opportunities for Research in Information Systems and Information Technology*, 22 J. GLOBAL INFO. TECH. MGMT. 4, 235–242 (2019).

<sup>12</sup> Geoffrey M. Hodgson, *Taxonomic Definitions in Social Science, with Firms, Markets and Institutions as Case Studies*, 15 J. INST. ECON. 207, 212–13 (2019).

13. To understand this point, recall from my opening report (at ¶¶ 30–40) that not all blockchains share an identical basic architecture. Bitcoin is an example of a proof-of-work blockchain. (Expert Report of Peter Adriaens (Oct. 4, 2021) (“Adriaens Report”) at 17.) The current state of Ethereum is another example of a proof-of-work blockchain (though, as Dr. [REDACTED] recognizes, Ethereum is transitioning to a different model known as proof of stake).

The XRP Ledger uses neither proof-of-work nor proof of stake, but rather a federated consensus model.<sup>13</sup> Dr. [REDACTED] use of the four factors he selects depends on an assumption that they provide a reliable way to assess, objectively test, quantify, or compare substantively distinct blockchain architectures. That assumption is flawed. First, as the Troncoso paper itself underscores, the criteria used to measure decentralization in a particular blockchain system must account for differences in **network infrastructure** (“the distribution of tasks needed for maintaining service within the system”), **network topology** (“the connections between nodes used to route traffic”), and **authority topology** (“the power relations between the nodes”), lest they ignore important differences in how different blockchains realize or achieve decentralization in practice.<sup>14</sup> Dr. [REDACTED] report does not address this.

14. An example helps to illustrate the importance of having reliable mechanisms to compare substantively different architectures before reaching useful conclusions. For decades, “miles per gallon” (MPG) was a reliable mechanism for comparing the efficiency of two different cars, and an observer who was only aware of gasoline-powered cars might therefore assume that all cars can be assigned an MPG measurement. If, however, that observer were then introduced to a Tesla, which does not run on gasoline and cannot be assigned an MPG, the measurement

---

<sup>13</sup> See *Consensus Protections Against Attacks and Failure Modes*, XRPL.ORG, <https://xrpl.org/consensus-protections.html>.

<sup>14</sup> See Troncoso et al., *supra* note 2, at 309–13, 320.

criterion would fail to recognize the Model 3 as a car, because it failed to account for differences in the underlying architecture.

15. Dr. [REDACTED] assumption that his four selected criteria can be reliably applied to assess and compare Bitcoin, Ethereum, and the XRP Ledger is further flawed because it does not consider decentralization at various *layers* of those three blockchain systems. A recent review on the taxonomy of metrics to characterize and measure (de)centralization indicates that the techniques that are useful depend on the layer in the blockchain one wants to compare, and on the particular blockchain architecture at issue.<sup>15</sup> Whereas the subsystems (or “layers”) are defined differently between Srinivasan and Lee<sup>16</sup> or Sai, the results in Chart 1, taken from Sai, indicate that multiple techniques are favored.<sup>17</sup> Sai identifies a total of 13 aspects spread over six architectural layers that are relevant to the issue of decentralization in public blockchains – and for several of those aspects, Sai observes that no measurement techniques can even be found yet within the literature (see the “Not found” notations in Chart 1).<sup>18</sup>

| Layer             | Centralization factor               | Measurement techniques  |
|-------------------|-------------------------------------|---|
| Application layer | Wallet concentration                | Not found   |
|                   | Exchange concentration              | Centrality & Percentage value   |
|                   | Reference client concentration      | Satoshi index   |
| Operational layer | Storage constraint                  | Ratio of growth   |
|                   | Specialized equipment concentration | Not found   |
| Incentive layer   | Wealth concentration                | Gini coefficient & Percentage value                                       |
| Consensus layer   | Consensus power distribution        | Percentage value & Gini coefficient & Theil index & Centralization factor |
| Network layer     | Node discovery protocol control     | Not found   |
|                   | Geographic distribution             | Gini coefficient & Latency  |
|                   | Bandwidth concentration             | Clustering of provisioned bandwidth                                       |
|                   | Routing centralization              | AS-Level coverage   |
| Governance layer  | Owner control                       | Fractional measurement  |
|                   | Improvement protocol                | Centrality metrics  |

Chart 1. Decentralization metrics considered across blockchain layers (from Sai et al., 2021)

<sup>15</sup> Sai et al., *supra* note 4, at 5, 12–28.

<sup>16</sup> Balaji S. Srinivasan & Leland Lee, *Quantifying Decentralization*, EARN.COM (July 27, 2017), <https://news.earn.com/quantifying-decentralization-e39db233c28e>.

<sup>17</sup> Sai et al., *supra* note 4, at 12.

<sup>18</sup> *Id.*

16. The active study of decentralization factors – and the development of appropriate metrics and techniques to measure them – in the scientific literature indicates an on-going need for research to compare blockchains, and demonstrates that this area is unsettled, and that there is currently no standard or benchmark for use in the profession.<sup>19</sup> This observation is exemplified in Chart 1 by measurement techniques labeled “Not found,” indicating that even as to factors relating to decentralization that have been proposed, there is no reliable way to measure or objectively assess different blockchains as to those factors.

17. By way of further example, a 2020 study called “Measuring Decentrality in Blockchain Based Systems” emphasizes the need to measure decentralization at different layers of the system, using “various metrics” to capture decentrality in “respective layers.”<sup>20</sup> For measuring decentrality at the governance layer (the layer in which the nodes reach a consensus), the authors propose using seven different metrics including: “fairness index, entropy, Gini coefficient, Euclidean distance, Minkowski distance, cosine similarity and Kullback-Leibler divergence metrics.”<sup>21</sup> I express no view on whether those seven metrics are the right ones or not – as this is an emerging area of study lacking consensus on approach – but it is striking that the prevailing literature is both layer-sensitive and architecture-sensitive in proposing metrics, whereas Dr. [REDACTED] approach is not.

18. Hence, the differences in incentive, governance, operational, and validation mechanisms (proof-of-work for Bitcoin and Ethereum; federated consensus for the XRP Ledger) do not allow

---

<sup>19</sup> See *id.* at 5 (explaining that the “study of centralization in public blockchain is still fragmented” and current models “do not provide adequate insights,” therefore setting out to design a “novel centralization taxonomy” to “overcome th[at] limitation”).

<sup>20</sup> Sarada Prasad Gochhayat et al., *Measuring Decentrality in Blockchain Based Systems*, 8 IEEE ACCESS 178372, 178376 (2020).

<sup>21</sup> *Id.* at 178373.

for a direct metrics comparison on the same basis. Given there is no consensus in the literature and the practice to measure these metrics objectively **at the subsystem or layer** evaluated, there is a lack of methodology and process to compare **entire blockchains** at a systems level. Dr.

██████ does not acknowledge this lack of consensus, nor does he offer a basis to conclude that his novel four-factor framework is (or is based on) a generally accepted methodology.

**C. There are no accepted metrics to use to quantify whether a given ledger satisfies criteria for decentralization, especially for purposes of comparing Bitcoin, Ethereum and the XRP Ledger.**

19. In addition, to the extent that Dr. ██████ identifies a series of criteria that he asserts are relevant to whether a particular blockchain is decentralized, he does not substantiate – and the relevant literature does not provide – metrics by which one may reliably and consistently quantify the four criteria in question. I will address each of the four in turn.

20. **Resilience (Nakamoto Coefficient).** The concept of resilience is often described as a major benefit of blockchains, and it refers generally to a blockchain’s persistence in moving forward in a trusted way and ability to withstand challenges such as hacking, malware, fraud, server or network failure, and human error. Dr. ██████ report decides to assess and measure Resilience across the Bitcoin, Ethereum, and XRP Ledger systems using a metric he calls the “Nakamoto Coefficient” – “the number of parties that need to be corrupted to subvert key properties of a distributed system.” (Report at 5 n.1.) I am not aware of any peer-reviewed literature that considers the Nakamoto Coefficient, as a term or as defined by Dr. ██████ as a suitable or accepted metric for measuring the decentralization of a blockchain. Dr. ██████ cites

a (non-peer-reviewed) YouTube video and blog post in relying on the concept of a Nakamoto Coefficient for this purpose.<sup>22</sup>

21. The blog post Dr. [REDACTED] cites explains that calculating the Nakamoto Coefficient requires that one:

- (a) enumerate the essential subsystems of a decentralized system,
- (b) determine how many entities one would need to be compromised to control each subsystem, and (c) then use the minimum of these as a measure of the effective decentralization of the system. The higher the value of this minimum Nakamoto Coefficient, the more decentralized the system is.<sup>23</sup>

22. That post concludes by stating that the authors “recognize that there is plenty of room for debate over which subsystems of a decentralized system are essential.”<sup>24</sup> Dr. [REDACTED] does not offer, and I am not aware of, any basis to conclude that the debate around identifying essential subsystems that these authors acknowledge has been resolved in favor of considering solely “safety” and “liveness,” which Dr. [REDACTED] asserts are the two principal properties of Resilience. (Report at 9.) Indeed, neither word appears anywhere in the blog post that defined the Nakamoto Coefficient (nor do the

---

<sup>22</sup> Stacks, Balaji Srinivasan of 21: “Quantifying Decentralization” Blockstack Summit 2017, YOUTUBE (Aug. 11, 2017), <https://www.youtube.com/watch?v=4UXT5YVJwB4>. The YouTube video in question, *Quantifying Decentralization*, is related to a blog post on Earn.com by the same author. Srinivasan & Lee, *supra* note 16. Later in his report, Dr. [REDACTED] defines Resilience as the ability of a system “to withstand Byzantine behavior of components of the system.” (Report at 9.) He then states that Resilience “may apply to different properties of the system, namely safety and liveness,” which he defines as the properties of a system that bad things do not happen (safety) and good things do eventually happen (liveness). (*Id.*) Dr. [REDACTED] again offers no citation for this notion. For the reasons explained later in this report, none of this supplies a reliable metric for measuring blockchain systems’ decentralization.

<sup>23</sup> Srinivasan & Lee, *supra* note 16.

<sup>24</sup> *Id.*



words “double-spend resistance” or “censorship,” which Dr. [REDACTED] uses as examples of safety and liveness properties).

23. Rather, the authors of that post calculate the Nakamoto Coefficient by drawing on two concepts from economic theory – the Lorenz curve and the Gini coefficient – which itself was a leap by the (non-peer-reviewed) post’s authors.<sup>25</sup> The Lorenz curve and the Gini coefficient were originally designed to measure non-uniformity within a population.<sup>26</sup> Originally defined as a measure of the distribution of income across a population, the Gini coefficient is often used as a gauge of economic inequality, measuring income distribution or, less commonly, wealth distribution among a population.<sup>27</sup> The application of the Gini coefficient to analyze inequality in internet communities such as blockchains is flawed because it conflates two different problems: lack of resources and concentration of power.<sup>28</sup> These aspects should be considered separately since resource allocation is a network-dependent feature and power concentration is a feature of allocation of tokens. Absent a basis to conclude that allocation of tokens corresponds to authority, power, or control over a blockchain’s functioning, there is no basis to conclude that

---

<sup>25</sup> *Id.*

<sup>26</sup> UNITED STATES CENSUS BUREAU, *Gini Index*, <https://www.census.gov/topics/income-poverty/income-inequality/about/metrics/gini-index.html> (last revised Oct. 8, 2021) (explaining that the Gini coefficient “summarizes the dispersion of income across the entire income distribution,” “based on the difference between the Lorenz curve (the observed cumulative income distribution) and the notion of a perfectly equal income distribution”).

<sup>27</sup> *Id.*; see generally Oded Stark, *Status Aspirations, Wealth Inequality, and Economic Growth*, 10 REV. DEV. ECON. 171 (2006) (utilizing a Gini coefficient of wealth inequality in suggesting how such inequality corresponds to economic growth).

<sup>28</sup> Compare Srinivasan & Lee, *supra* note 16 (describing the Nakamoto coefficient as a measure of the number of entities needed to control a subsystem, inspired by the Gini coefficient and Lorenz curve), with Frank A. Farris, *The Gini Index and Measures of Inequality*, 117 AM. MATHEMATICAL MONTHLY 851 (2010) (describing the Gini index as a “single number that measures how equitably a resource is distributed in a population”).



token allocation is relevant to decentralization. (I further address this point below, when considering Dr. ██████ definition of Governance.)

24. In addition, the Nakamoto Coefficient (like the Lorenz curve and Gini coefficient on which it is based; *see* Chart 2) is designed to measure the distribution of scarce resources (originally, money) within a defined population.<sup>29</sup> Accordingly, it is only a valid analytical tool to the extent it is analyzing a scarce resource (in economic theory, money) whose distribution has some relationship to the distribution of power within the system (for example, buying power).

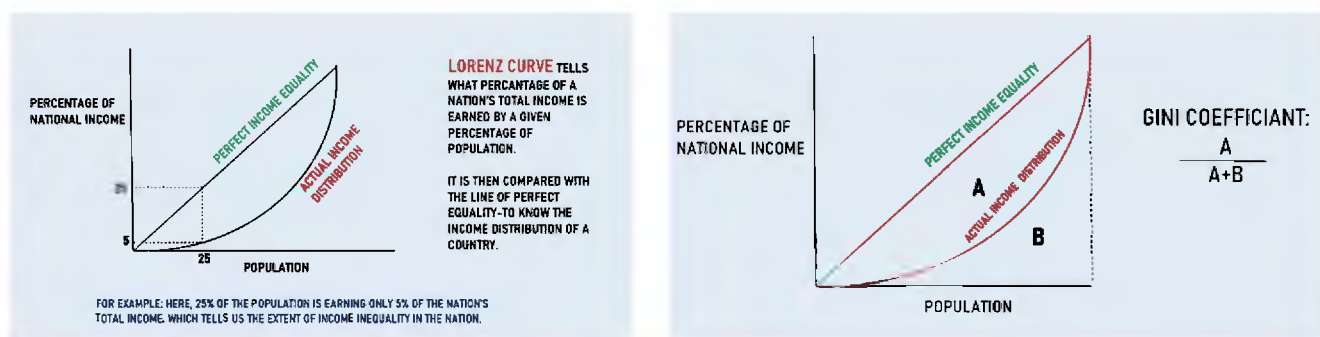


Chart 2. Illustration of Lorenz Curve and Gini Coefficient.<sup>30</sup>

25. Even if the concept of the Nakamoto Coefficient that was proposed by this non-peer reviewed blog post were reliable, Dr. ██████ application of the Nakamoto Coefficient to the XRP Ledger rests on an undefended logical leap. In particular, he overlooks the fact that the XRP Ledger uses a completely different consensus mechanism – one that *does not* use scarce resources to allocate authority. Rather, it permits each participant to independently choose which other participants to trust, as each validator has complete control over the contents of its Unique Node List, which a validator may change at any time without needing the permission of any other party. As a consequence, I do not believe that the Nakamoto Coefficient can be

<sup>29</sup> Srinivsan & Lee, *supra* note 16.

<sup>30</sup> Arsh, *What are the Main Merits of the Lorenz Curve?*, QUORA (2021), <https://www.quora.com/What-are-the-main-merits-of-the-Lorenz-curve>.

sensibly applied to evaluate the XRP Ledger's Resilience. At a minimum, Dr. [REDACTED] has failed to defend his application of that metric.

26. In the context of Bitcoin and Ethereum, the scarce resource Dr. [REDACTED] measures is mining power, which is relevant because of the authority given to successful miners in proof-of-work blockchain systems who may propose new blocks and the ability of a miner or miners that control the majority of the hash rate to undermine the validity of the system (in what is referred to as a "51% attack").<sup>31</sup> I therefore agree that Dr. [REDACTED] decision to apply the Nakamoto Coefficient to Bitcoin and Ethereum to determine the distribution of mining power across the network is reasonable. But I do not agree that Dr. [REDACTED] offers a complete analysis of the Nakamoto Coefficient's application. The nature of the Nakamoto Coefficient is that it can only offer a point-in-time result: in other words, just as the Gini coefficient of the United States changed from 1920 to 1950 to 1990 to 2020, the Nakamoto Coefficient of Bitcoin and Ethereum is not static.<sup>32</sup> It is public knowledge that mining-power concentrations have changed over time for Bitcoin and Ethereum.<sup>33</sup> And Dr. [REDACTED] report recognizes that he is calculating the Nakamoto Coefficient of Bitcoin and Ethereum by measuring the concentrations of mining power "at the time of writing this report." (Report at 15.) That is insufficient to reach any conclusions about the blockchains themselves, and could only (and at most) permit an analysis of

---

<sup>31</sup> See Digital Currency Initiative, *51% Attacks*, MIT MEDIA LAB, <https://dci.mit.edu/51-attacks> (last visited Nov. 11, 2021).

<sup>32</sup> See, e.g., Juliana Horowitz et al., *Trends in Income and Wealth Inequality*, PEW RSCH. (Jan. 9, 2020), <https://www.pewresearch.org/social-trends/2020/01/09/trends-in-income-and-wealth-inequality>.

<sup>33</sup> See e.g., Cambridge Centre for Alternative Finance, *Bitcoin Mining Map*, U. CAMBRIDGE, [https://ccaf.io/cbeci/mining\\_map](https://ccaf.io/cbeci/mining_map) (last visited Nov. 11, 2021); ETHERSCAN, *Ethereum Network Hash Rate Chart*, <https://etherscan.io/chart/hashrate> (last visited Nov. 11, 2021).

the relative ownership of scarce resources by the participants in each blockchain's network at a given point in time.

27. An objective analysis of the Nakamoto Coefficients of Bitcoin and Ethereum based on Dr. [REDACTED]'s own definition – the minimum number of parties that need to be corrupted to subvert key properties of the systems (Report at 5 n.1) – would necessarily conclude that the Nakamoto Coefficients of both systems are no greater than 1 as to the two features of Resilience that Dr. [REDACTED] identifies: **safety** (that “‘bad things’ do not happen (Report at 9)) and **liveness** (that “‘good things’ do eventually happen” (*id.*)).

28. As to safety, an example of which Dr. [REDACTED] gives as double-spend resistance, both Bitcoin and Ethereum are vulnerable, as Dr. [REDACTED] recognizes, to a “51% attack.” (Report at 15, 18.) If one entity controls 51% of the hash power of the network, they are able to compromise the safety of the entire network.<sup>34</sup>

29. As to liveness, an example of which Dr. [REDACTED] gives as censorship resistance (Report at 9), both Bitcoin and Ethereum grant successful miners complete discretion to censor or reject transactions.<sup>35</sup> Accordingly, a single miner (even without 51% of the hash rate) has the ability to void a proposed transaction for any reason without any oversight.<sup>36</sup> For the user who proposed

---

<sup>34</sup> This degree of control over the Bitcoin hash rate has occurred, albeit briefly, in the past. See Alex Hern, *Bitcoin Currency Could have been Destroyed by '51%' Attack*, THE GUARDIAN (June 16, 2014), <https://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io>.

<sup>35</sup> Andreas M. Antonopoulos, *MASTERING BITCOIN* 275 (2d ed. 2017); Johnnatan Messias et al., *On Blockchain Commit Times: An Analysis of How Miners Choose Bitcoin Transactions*, in PROC. OF THE SECOND INT’L KDD WORKSHOP ON SMART DATA FOR BLOCKCHAIN AND DISTRIBUTED LEDGER, 3–4 (Aug. 2020), <https://people.mpi-sws.org/~johnme/pdf/messias-sdbd-20.pdf>.

<sup>36</sup> See Hern, *supra* note 3426.

the voided transaction, there is no in-network recourse other than resubmitting the transaction, which does not satisfy Dr. [REDACTED] definition of liveness.<sup>37</sup>

30. **Inclusiveness.** Dr. [REDACTED] defines inclusiveness (solely by citation to his own, unpublished manuscript, which refers to the concept as “openness”) as “the ability of the system to welcome new participants in a way which provides them with equal opportunities compared to existing participants.” (Report at 9.) Dr. [REDACTED] then defines the concept of “equal opportunities” (again solely by citation to his own, unpublished manuscript) as a system that “(a) allows any participant Alice to have an equal role in the system as any other (new or existing) participant Bob, provided Alice makes the same investment in system resources as Bob, and (b) the system does not prevent Alice from making such an investment.” (Report at 9.)

31. Again, I find Dr. [REDACTED] methodology to be flawed. Dr. [REDACTED] report does not substantiate the relationship between “Inclusiveness” and decentralization. The report does not offer any citation to authoritative literature that describes Inclusiveness (or the sub-defined concept of equal opportunities) as necessary to determining whether a system is decentralized.

32. Even assuming that “Inclusiveness” is an appropriate criterion for evaluating decentralization, Dr. [REDACTED] report again offers no metrics that would permit one to reach conclusions about the significance of greater or lesser degrees of Inclusiveness in particular layers of distinct blockchain models.<sup>38</sup> Accordingly, even if Dr. [REDACTED] could substantiate his

---

<sup>37</sup> This censorship authority has been deployed in practice. See Collin Harper, *Marathon Miners Have Begun Censoring Bitcoin Transactions*, COINDESK (May 7, 2021), <https://www.coindesk.com/tech/2021/05/07/marathon-miners-have-started-censoring-bitcoin-transactions-heres-what-that-means/>.

<sup>38</sup> Dr. [REDACTED] report asserts that Inclusiveness may relate to whether a particular blockchain is *permissioned* or *permissionless*, but offers no analysis or citation to conclude – as he asserts – that “permissionless systems are to be considered more decentralized than permissioned systems.” (Report at 9.) Indeed, the simple example of the U.S. dollar refutes the premise: the dollar is a permissionless currency to access and

assertions, the failure to supply meaningful comparison metrics or benchmarks is an independent reason that his conclusions are impossible to trust or validate objectively.

33. Dr. [REDACTED] criterion of “equal opportunities” appears to be based only on [REDACTED], [REDACTED].<sup>39</sup> For Dr. [REDACTED] to assert that Bitcoin and Ethereum provide “equal opportunities” to participants, but the XRP Ledger does not, is particularly problematic. The literature has, for at least the past few years, been critical of Bitcoin and proof-of-work blockchains because the significant costs of mining and the manner in which the in-protocol incentives favor those with massive computing power, such that in practice “only a few nodes are contributing blocks for the Blockchain.”<sup>40</sup> Dr. [REDACTED] does not address this literature, which explains that it is insufficient to consider abstract equality of opportunity when structural barriers

---

spend, but is issued and controlled by a centralized authority (the U.S. government). INVESTOPEDIA, *See Who Prints Money in the United States?*, <https://www.investopedia.com/ask/answers/082515/who-decides-when-print-money-us.asp> (last updated May 29, 2021).

Similarly, as noted above, blockchains contain multiple functional layers. It is possible for a blockchain to be permissioned as to certain layers and permissionless as to others (for example, one blockchain might have a permissioned code base but permissionless transaction proposal and validation; another might have permissionless governance through a decentralized autonomous organization (DAO) model but have permissioned transactions).

39

40

[REDACTED]

Gochhayat et al., *supra* note 20, at 178381; *see also id.* at 178374 (“Despite envisioned decentralization in Bitcoin, the high cost of mining has led to considerable centralization of consensus in practice”); Sai et al., *supra* note 4, at 29 (“A high concentration of consensus power can induce an arm’s race to attain the most efficient hardware. Our survey reports that this race often results in specialized proprietary hardware. The practical implication of this type of hardware concentration is an indirect limitation to participation as only efficient, and often proprietary hardware, can result in a profitable operation.”); Gencer et al., *supra* note 9, at 9–11 (noting “[w]ith the current mining difficulty of Bitcoin and Ethereum, using commodity hardware to generate blocks is not feasible which centralizes the mining process somewhat,” and finding that in the ten week study period four Bitcoin miners had more than 53% of the average mining power and three Ethereum miners had 61% of average mining power).

prevent new entrants from meaningfully contributing to the system.<sup>41</sup> By contrast, operating a fully functioning validation server on the XRP Ledger requires minimal computing power.<sup>42</sup> As Dr. ██████ report fails to recognize, any person or entity may operate an XRP Ledger validation server and participate in the consensus process without the permission or approval of any other entity – exactly the type of equal opportunity his report defines as key to Inclusiveness. (Report at 9.)

34. **In-Protocol Incentives.** Dr. ██████ defines Incentives as “whether the system has rewards for protocol participants, paid out to protocol participants within the protocol itself.” (Report at 10.) To support his definition, and the relevance of Incentives to decentralization, Dr. ██████ relies on the Sai and Troncoso papers.<sup>43</sup> However, neither paper supports Dr. ██████ conclusions.

35. Sai et al. discuss the “incentive layer” of blockchains by observing that whether Bitcoin (and, by extension, Ethereum) actually offers economic incentives to its participants is contingent on factors external to the system. Specifically, if “the exchange rate” of Bitcoin to fiat currency “falls below a given threshold of profitability” it no longer provides an economic incentive and participants may withdraw from mining.<sup>44</sup> Put another way, if the cost of mining (measured by the cost of obtaining and operating the computing equipment) over any given

---

<sup>41</sup> Sai et al., *supra* note 4, at 22 (“[T]he specialized equipment requirement severely contains . . . participation.”); Igor Makarov & Antoinette Schoar, *Blockchain Analysis of the Bitcoin Market*, 23 (Oct. 13, 2021), <https://ssrn.com/abstract=3942181> (“[T]he set of large miners is relatively stable, and it is small miners which enter and leave the mining business in response to price shocks.”).

<sup>42</sup> *System Requirements: Minimum Specifications*, XRPL.ORG, <https://xrpl.org/system-requirements.html> (“A rippled server should run comfortably on commodity hardware”).

<sup>43</sup> See Report at 10 (citing Sai et al., *supra* note 4; Troncoso et al., *supra* note 2).

<sup>44</sup> Sai et al., *supra* note 4, at 19.

period is greater than the mining rewards received, the network does not effectively offer economic incentives.<sup>45</sup>

36. Dr. [REDACTED] asserts that the Troncoso paper “argue[s] that the development of adequate incentives is necessary to build a successful decentralized system.” (Report at 10.) However, the conclusions of Troncoso et al. do not support Dr. [REDACTED] assertion. To the contrary, the Troncoso paper concludes that Incentives (1) need not be economic, and (2) may in fact undermine decentralized systems if not constructed carefully: “Designers of decentralized systems must carefully engineer such incentives, to ensure that natural (non adversarial) selfishness does not lead to dysfunction. *Monetary incentives, reputation, and reciprocity can be the basis of such incentives – but off the shelf such mechanisms are often central points of failure.*”<sup>46</sup> Dr. [REDACTED] ignores this essential aspect of the Troncoso paper’s analysis when he asserts that Incentives must be “in-protocol” to be significant. (Report at 10.<sup>47</sup>) Instead, Dr. [REDACTED] report narrowly focuses on rewards earned through the energy and cost-intensive mining process (Report at 10, 16), and he ignores the XRP Ledger’s inherent structural and design benefits, including the ability to quickly, efficiently, and cheaply transfer value, which I detailed in my opening report. (Adriaens Report at 22, 25.) Each of these features of the XRP

---

<sup>45</sup> According to public reports, the exchange rate of Bitcoin has fallen to levels that rendered mining unprofitable in the past. See Evelyn Cheng, *Bad News for Bitcoin Miners: It’s No Longer Profitable to Create the Cryptocurrency*, by Some Estimates, CNBC (Mar. 15, 2018), <https://www.cnbc.com/2018/03/15/bad-news-for-bitcoin-miners-as-its-no-longer-profitable-to-create-the-cryptocurrency.html>.

<sup>46</sup> Troncoso et al., *supra* note 2, at 313 (emphasis added).

<sup>47</sup> A related problem with Dr. [REDACTED] argument is that he does not explain why it is sufficient that Bitcoin and Ethereum provide “in-protocol incentives” solely to miners, when he defines this aspect of his analysis as relating to “whether the system has rewards for protocol participants.” (Report at 10.) Miners are far from the only participants in the Bitcoin and Ethereum ecosystems; for other participants – like those who submit transactions and must pay a fee to miners – there are either no incentives or economic disincentives.



Ledger offer incentives – for example, to payment processors who want to ensure their transactions clear more quickly and cheaply than on the Bitcoin or Ethereum blockchains and therefore have an incentive to ensure the XRP Ledger continues to exist.

37. Moreover, the Troncoso paper observes that “[s]ome decentralized system[s] consist solely of nodes that are users and there is no additional infrastructure. They rely solely on users to collectively contribute resources (bandwidth, storage) in order to provide a service.”<sup>48</sup>

Troncoso labels such a system decentralized, even though there are no Incentives provided.<sup>49</sup>

38. Dr. [REDACTED] also offers no methodology or metrics to quantify the significance or adequacy of incentives in order to reliably compare the incentives offered by distinct blockchain architectures. This renders it impossible to validate his results. Nor does Dr. [REDACTED] account for issues considered by the literature, like the fact that the “in-protocol incentives” offered by Bitcoin and Ethereum are only economic incentives if external factors align correctly.<sup>50</sup>

39. Although Dr. [REDACTED] concludes that the XRP Ledger does not provide incentives because it has no equivalent to mining rewards, Dr. [REDACTED] never considers other forms of incentives identified by Troncoso – like reputation and reciprocity.<sup>51</sup> Indeed, reputation and reciprocity can form significant incentives in the context of distributed systems, as communities that see value in an innovative technological solution may be inclined to support them regardless of whether the solution offers “in-protocol” incentives.<sup>52</sup> As I set out in my original Report and

---

<sup>48</sup> Troncoso et al., *supra* note 2, at 310.

<sup>49</sup> *Id.* Troncoso refers to these systems as “decentralized” and lists Freenet and Cachet as examples, neither of which offer incentives. *See e.g.*, FREENET, <https://freenetproject.org/index.html>.

<sup>50</sup> *See supra* at ¶ 35.

<sup>51</sup> Troncoso et al., *supra* note 2, at 313.

<sup>52</sup> *See, e.g., Incentives to Develop Free Software*, THE LINUX INFORMATION PROJECT, [http://www.linfo.org/open\\_source\\_development\\_incentives.html](http://www.linfo.org/open_source_development_incentives.html) (listing ten reasons why



discuss further *infra* in Part III, the XRP Ledger offers many such innovative technological advances that would provide non-economic yet meaningful incentives.

40. **Governance.** Dr. [REDACTED] final criterion for evaluating decentralization is Governance, which he defines in two distinct ways in different places in his report. First, in his summary and Table 1, he identifies two aspects of Governance: public face, and tokens allocated at genesis. (Report at 5.) Second, in Section 3.1, he defines Governance as “the level of power, if any, of human stakeholders to influence and change key rules in the system, e.g. through software updates.” (Report at 10–11.) He then notes three “parameters for evaluating decentralization of governance power” that have been “proposed or discussed in the literature” – namely: (1) improvement control (the number of developers contributing to the codebase), (2) existence of a public face (a personality or institution that is a representative of the system), and (3) owner control (measured by examining the total tokens accumulated by the stakeholders in the early adoption period). (Report at 11.) As with the other criteria Dr. [REDACTED] analyzes, the Governance criterion is not reliable both because it does not have an agreed-upon definition (as Dr. [REDACTED] admits in noting that the parameters he identifies have merely been “proposed or discussed” (Report at 11)), and because there is no agreed-upon metric for evaluating quantitatively any of the parameters he identifies in a manner that would permit comparisons across blockchains.

---

developers contribute to open-source projects, like the Linux operating system and the Internet itself, including the desire to use the system they are developing or maintaining, prestige, and profit from downstream businesses that contributors operate); Josh Lerner & Jean Tirole, *The Simple Economics of Open Source*, NAT’L BUREAU ECON. RSCH. (2000) [https://www.nber.org/system/files/working\\_papers/w7600/w7600.pdf](https://www.nber.org/system/files/working_papers/w7600/w7600.pdf) (concluding that future career advancement, peer recognition, and related incentives were powerful drivers behind the development of key software projects in the 1990s).

41. *Improvement Control.* Although not identified in Dr. [REDACTED] summary Table 1, he defines Improvement Control as relevant to Governance. (Report at 11.) According to Dr. [REDACTED] (Report at 16, 18), Bitcoin has “relatively few ‘core’ developers” and Ethereum is “largely similar” to Bitcoin in terms of improvement proposals – though the literature he cites indicates that, at least for Ethereum, one person – Vitalik Buterin – is the source of the “vast majority” of the code base.<sup>53</sup>

42. Also, Dr. [REDACTED] asserts that “the overwhelming majority of code commits and lines of code” in rippled “comes from the developers who are or have been affiliated with or funded by Ripple Labs, Inc.” (Report at 23.) Unlike the Azouvi paper Dr. [REDACTED] cites,<sup>54</sup> however, the Report offers no quantitative analysis to support those assertions, so it is not possible to determine, for example, whom he considers to be the “core” developers of Bitcoin or Ethereum, or a developer “affiliated with or funded by Ripple Labs, Inc.” (Report at 23.) Dr. [REDACTED] analysis in this regard is therefore not replicable.<sup>55</sup>

43. However, taking Dr. [REDACTED] assertions as true for the sake of argument, Dr. [REDACTED] offers no metrics to quantitatively measure Improvement Control such that it could be compared

---

<sup>53</sup> See, e.g., Sai et al., *supra* note 44, at 3 (“According to the empirical analysis of Azouvi et al. (2018), the authors report that the vast majority of the improvement proposal in Ethereum are authored by a single user, Vitalik Buterin, the founder of Ethereum.”).

<sup>54</sup> See Report at 11 (citing Azouvi et al., *supra* note 9).

<sup>55</sup> To support the proposition that Improvement Control is relevant to his decentralization aspects, Dr. [REDACTED] cites to a paper by de Filippi and Loveluck (Report at 11) that reports that five individuals who held “administration rights for the development of the Bitcoin project became known as the *core developers*.” Primavera de Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure*, 5 INTERNET POL’Y REV. 1, 9 (2016), <https://policyreview.info/pdf/policyreview-2016-3-427.pdf>. This fact further undermines Dr. [REDACTED] use of the term to refer to the top contributors to a particular blockchain project since the Bitcoin “core developers” were selected by Gavin Andresen and defined by the fact that they controlled the Bitcoin code, as discussed *infra* note 56.

across different blockchain systems (which is perhaps why Dr. [REDACTED] does not include this facet of Governance in his summary Table 1). Dr. [REDACTED] report lacks any reliable methodology to measure Improvement Control, making it impossible to use this parameter to evaluate Governance or any other aspect of decentralization.

44. *Public Face.* Dr. [REDACTED] asserts that Bitcoin has no “public face,” while Ethereum and the XRP Ledger do. (Report at 16, 18, and 23.) Dr. [REDACTED] conclusion in this regard as to Bitcoin is highly temporally contingent. As has been widely reported, early in Bitcoin’s development, a single individual – Gavin Andresen – was the principal developer of the Bitcoin software code, and worked with a small team of core developers to make the necessary improvements to Bitcoin that allowed it to flourish.<sup>56</sup> Similarly, as Dr. [REDACTED] acknowledges, Vitalik Buterin is responsible for the original design and development of Ethereum and remains its public face. (Report at 18.)

45. As with the other parameters he identifies, Dr. [REDACTED] offers no reliable metric to evaluate the Public Face of a particular blockchain, and no explanation of its relevance to the concept of decentralization as he (which is to say, Troncoso) defined it. The mere existence of a recognizable Public Face associated with a blockchain project has no apparent connection to whether “multiple authorities (parties) control different system components and no authority is

---

<sup>56</sup> Tom Simonite, *The Man Who Really Built Bitcoin*, MIT TECH. REV. (Aug. 15, 2014), <https://www.technologyreview.com/2014/08/15/12784/the-man-who-really-built-bitcoin/> (“When Andresen took over from Satoshi Nakamoto in 2010 he laid out the way the project would operate, drawing on his experience managing teams building software products and what he knew of major open source projects such as Linux. A group of five core developers emerged, with Andresen as the most senior. Only they had the power to change the code behind Bitcoin and merge in proposals from other volunteers. That gave them unique power over the currency’s basic operation and economic parameters. While the price of Bitcoin soared over the years, Andresen and the other core developers toiled to improve the software that made it all possible. They fixed security bugs that had permitted digital heists, made the software less prone to crashes, and spruced up the interface to make it easier to use.”).

fully trusted by all,” (Report at 5) (citing Troncoso et al., at 308), because it is entirely possible for those defined features to be met even where a single individual is responsible for the creation of the project. For example, Satoshi Nakamoto – the pseudonymous creator of Bitcoin – was clearly a significant contributor to the Bitcoin project, having developed its initial source code, but the actual governance and functioning of the blockchain is not impaired by his anonymity and lack of ongoing (known) support for the project.<sup>57</sup>

46. *Token Allocation at Genesis.* Finally, Dr. [REDACTED] asserts that the “total tokens accumulated by the stakeholders in the early adoption period” of a blockchain is a relevant parameter of Governance. (Report at 11.) As an initial matter, Dr. [REDACTED] offers no explanation for why control of a blockchain’s tokens (which are inherently solely units of account recorded on the blockchain) is relevant to whether the blockchain itself is decentralized. Except in a proof of stake blockchain (which none of Bitcoin, Ethereum, or the XRP Ledger are at present), ownership of tokens provides no mechanism to control the operations of the ledger, nor any obligation on others in the system to trust the token holder, and accordingly does not have relevance to the features of a decentralized system as Dr. [REDACTED] defines it. Nor does Dr. [REDACTED] offer any quantifiable metrics that would allow for a meaningful comparison of one blockchain project to another, even were one to accept the utility of this parameter.

47. Dr. [REDACTED] description of the Token Allocation at Genesis for Bitcoin, Ethereum, and XRP are also flawed as a factual matter.

48. As to Bitcoin, Dr. [REDACTED] asserts that 0% of the tokens were allocated at genesis and that “Bitcoin did not have a hidden owner accumulation phase.” (Report at 17.) Dr. [REDACTED] leaves

---

<sup>57</sup> Jamie Redman, *Ten Years Ago Satoshi Nakamoto Logged Off*, BITCOIN.COM (Dec. 13, 2020), <https://news.bitcoin.com/ten-years-ago-satoshi-nakamoto-logged-off-the-final-message-from-bitcoins-inventor>.

to a footnote, however, an acknowledgement of the widespread reports that wallets controlled by Bitcoin’s inventor, Satoshi Nakamoto, contain approximately 1.1 million BTC that were mined in the early days of the protocol.<sup>58</sup> Dr. [REDACTED] also acknowledges that those BTC “were never transacted on the network,” (Report at 17 n. 12), meaning that Nakamoto presumably still controls a sizeable percentage of BTC – 1.1 million out of the 21 million that can ever be created, which would be worth over \$70 billion today.<sup>59</sup>

49. As to Ethereum, Dr. [REDACTED] initially asserts in Table 1 that 61.5% of the current supply of ETH tokens were allocated at genesis, with about 10% “owner controlled.” (Report at 5.) Dr. [REDACTED] later acknowledges that 72 million ETH were pre-allocated in the genesis block (Report at 18–19), which would be about 61% of the approximately 118 million ETH in circulation today.<sup>60</sup> However, Dr. [REDACTED] calculation of the amount of originally mined ETH that was “owner controlled” fails to account for the fact that all ETH in the genesis block was effectively controlled by the ETH development team,<sup>61</sup> which sold a significant quantity of the pre-mined ETH to fund the development of the system (which Dr. [REDACTED] refers to as “the ICO” or Initial

---

<sup>58</sup> See Sergio Demian Lerner, *The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin Creator, Visionary and Genius*, BITSLOG, <https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/>.

<sup>59</sup> Based on an observed exchange rate of approximately 1 BTC = USD \$65,000. See CRYPTOCOMPARE, *Bitcoin (BTC) – USD*, <https://www.cryptocompare.com/coins/btc/overview/> (as observed Nov. 11, 2021).

<sup>60</sup> ETHERSCAN, *Ether Total Supply and Market Capitalization Chart*, <https://etherscan.io/stat/supply> (as observed Nov. 11, 2021) (reporting the total ether token supply as 117,783,769.76 ETH).

<sup>61</sup> CONSENSYS, *A Short History of Ethereum* (May 13, 2019), <https://consensys.net/blog/blockchain-explained/a-short-history-of-ethereum>; Luit Hollander, *History of Ethereum Hard Forks*, MYCRYPTO (May 4, 2020), <https://medium.com/mycrypto/the-history-of-ethereum-hard-forks-6a6dae76d56f> (describing how the Ethereum development team included the 8,893 pre-sale transactions in the Ethereum genesis block and manually set the gas limit for the first few days of the Ethereum blockchain’s existence).

Coin Offering of ETH).<sup>62</sup> Accordingly, a more accurate description of the Token Allocation of ETH is that the allocation of all 72 million was controlled by the owners at the beginning of the ICO, and the owners sold all but 10% to fund the development of the blockchain.<sup>63</sup>

### III. Additional Responses to Dr. [REDACTED] Report.

50. Dr. [REDACTED] at various places in his report, seizes upon the default Unique Node List (“dUNL”) present in the rippled software that underlies the XRP Ledger as grounds to conclude that the XRP Ledger as of October 2021 “is centralized” and that the dUNL is “a root cause of inequality in the system.” (Report at 22.) Dr. [REDACTED] states that the dUNL contains a list of “[p]articipants required for the proper operation of” the XRP Ledger. (Report at 6.) However, no participant in the XRP Ledger’s validation process is required to use the dUNL to participate in validation.<sup>64</sup> Indeed, as Dr. [REDACTED] observes, the code of the XRP Ledger itself identifies two alternative UNLs—neither published by Ripple—that are available for validators to use. (Report at 20.) That one UNL is the “default” within the rippled code does not establish that use of the dUNL is *required*.<sup>65</sup> Moreover, Dr. [REDACTED] willingness to conclude that the “issue of a centralized dUNL publisher, alone, is in my opinion sufficient to render the XRP Ledger centralized” (Report at 6), demonstrates the insufficiency of his analysis in light of the literature

<sup>62</sup> Vitalik Buterin, *Launching the Ether Sale*, ETHEREUM FOUNDATION BLOG (July 22, 2014), <https://blog.ethereum.org/2014/07/22/launching-the-ether-sale>.

<sup>63</sup> Camila Russo, *Sale of the Century: The Inside Story of Ethereum’s 2014 Premine*, COINDESK (July 11, 2020), <https://www.coindesk.com/markets/2020/07/11/sale-of-the-century-the-inside-story-of-ethereums-2014-premine>.

<sup>64</sup> See *FAQ: What are Unique Node Lists (UNLs)?*, XRPL.ORG, <https://xrpl.org/faq.html> (“Each server operator can choose their own UNL.”).

<sup>65</sup> See *FAQ: Which UNL Should I Select?*, XRPL.ORG, <https://xrpl.org/faq.html> (“Currently, three publishers (Ripple, the XRP Ledger Foundation, and Coil) are known to publish recommended default lists of high quality validators, based on past performance, proven identities, and responsible IT policies. However, **every network participant can choose which validators it chooses as reliable and need not follow one of the three publishers noted above.**” (emphasis added)).



in the field. I am not aware of any peer-reviewed paper, and Dr. [REDACTED] cites none, that suggests that it is sufficient to examine one aspect of one layer of a blockchain and reach a conclusion as to whether the blockchain itself is centralized. To the contrary, the literature (including, but not limited to, Sai et al.) makes clear that a more thorough analysis is necessary before it is appropriate to draw any global conclusions regarding centralization, and further recognizes that not all layers of a blockchain must be fully decentralized for the blockchain to be considered decentralized on the whole.<sup>66</sup>

51. Dr. [REDACTED] also draws extensively from a 2018 paper by Chase and MacBrough (which was not peer-reviewed) to argue – without any independent analysis by Dr. [REDACTED] himself to substantiate the paper’s conclusions – that a high amount of overlap is required between different validators’ UNLs for the XRP Ledger to “provide” safety and liveness and for the “correct operation” of the XRP Ledger.<sup>67</sup> (Report at 21–22 and Appendix B.) Dr. [REDACTED] report, in turn, seizes on this overlap to opine that the XRP Ledger is centralized. (Report at 22.) I offer a few responses.

52. As an initial matter, Dr. [REDACTED] reliance on the Chase and MacBrough paper is misplaced because his report and the Chase and MacBrough paper analyze different versions of the rippled code. The research by Chase and MacBrough was performed as of February 21,

---

<sup>66</sup> Sai et al., *supra* note 4, at 29–30; *see also*; Steven Ehrlich, *Do Crypto and Blockchain Need To Be Decentralized To Succeed In 2019?*, FORBES (Dec. 17, 2018), <https://www.forbes.com/sites/stevenehrlich/2018/12/17/do-crypto-and-blockchain-need-to-be-decentralized-to-succeed-in-2019/?sh=55d667034442>.

<sup>67</sup> Notably, Chase and MacBrough make clear that their analysis only addresses the question of what might be necessary to “guarantee correctness” – not what is necessary for the XRP Ledger to function or operate. Brad Chase & Ethan MacBrough, *Analysis of the XRP Ledger Consensus Protocol 2* (Feb. 21, 2018), <https://arxiv.org/abs/1802.07242>. As Dr. [REDACTED] report admits, neither Bitcoin nor Ethereum guarantee correctness under any conditions, as they are always vulnerable to a 51% attack. (Report at 15, 18.)

2018, apparently based upon a 2018 version of the rippled code.<sup>68</sup> In contrast, Dr. [REDACTED] says he looked at the “current” version of the rippled code in effect as of the date of his report – October 4, 2021. (Report at 7.) It would therefore be unsound for Dr. [REDACTED] to base his analysis or conclusions of the “current” rippled code upon a study that looked at a version of the software that is more than three years out of date. In that regard, the history of changes to the rippled code (which is open source and public) indicates that significant changes to the code have occurred between 2018 and the present.<sup>69</sup> Dr. [REDACTED] offers no basis to establish that the Chase and MacBrough analysis, nor his own conclusions based on Chase and MacBrough, are still valid more than three years after that paper was released and after multiple updates to the rippled software that modified the consensus mechanism on which Dr. [REDACTED] grounds his opinions.

53. Dr. [REDACTED] also does not consider that federated consensus models inherently require human agreement – the selection of a list of trusted validators – as a basic element, yet no peer-reviewed or other literature suggests or states that federated consensus blockchains are always centralized or cannot be decentralized. This is a limitation of Dr. [REDACTED] “Governance”

---

<sup>68</sup> According to Github, which contains the history of the open-source rippled code, version 0.90.0 of rippled was released on February 20, 2018. Assuming that Chase and MacBrough did not complete their article in a single day, it is likely that they were referring to an even earlier version of the rippled code, such as version 0.81.0 (released February 2, 2018) or version 0.80.2 (released December 15, 2017). *See Releases - rippled*, <https://github.com/ripple/rippled/releases>.

<sup>69</sup> Rippled version 0.90.0 contains “several features and enhancements that improve the reliability, scalability and security of the XRP Ledger.” *Rippled Version 0.90.0*, GITHUB, <https://github.com/ripple/rippled/releases/tag/0.90.0>. Rippled version 1.6.0 “introduces several new features including changes to the XRP Ledger’s consensus mechanism to make it even more robust in adverse conditions,” including changes that “can improve the liveness of the network during periods of network instability.” *Rippled (XRP Ledger server) Version 1.6.0*, GITHUB, <https://github.com/ripple/rippled/releases/tag/1.6.0>. Both of these versions of rippled were released between the version considered by Chase and MacBrough and the version considered by Dr. [REDACTED]



analysis that means he is unable to conduct a comparison between the XRP Ledger and proof-of-work systems (e.g. Bitcoin and Ethereum).

54. Dr. ██████ report concludes by purporting to analyze “[w]hat risks to the XRP Ledger would or might materialize if Ripple ‘walked away’ or ‘disappeared.’” (Report at 25.) As an initial matter, Dr. ██████ cites no authority – and I am aware of none – to establish a methodology for such an analysis in the blockchain context. Dr. ██████ analysis is purely speculative, grounded in unsupported assumptions about the behavior of multiple parties within the XRP Ledger ecosystem, and cannot form the basis for a reliable or repeatable conclusion. For example, Dr. ██████ asserts that universities who have received funding from Ripple in the past may cease to operate validators if Ripple’s funding disappeared. (Report at 26.) Dr. ██████ offers no support for this assumption, and given the exceedingly low cost of operating a validator,<sup>70</sup> there is ample basis to believe Dr. ██████ assumptions could prove incorrect.

55. Dr. ██████ assumptions about what might happen if Ripple disappears are subjective and based on the assumption that the current state of the XRP Ledger predominantly or entirely contains validator nodes that use Ripple’s dUNL. This assumption is visible in assertions like “[i]n the case where more than 20% of validators in the dUNL disappear, the network would not be operational. The current dUNL (as of October 4, 2021) contains 41 validators . . . . Hence, the network would cease to be operational if nine validators disappeared.” (Report at 26.) Dr. ██████ never establishes as a matter of fact, however, that the current operational XRP Ledger validators actually use the current dUNL, such that 20% of current dUNL validators disappearing could impact the operation of the network. As Dr. ██████ acknowledges, two other UNLs that are not published by Ripple exist and, indeed, are referenced in the rippled code base. (Report at

---

<sup>70</sup> See *supra* note 42.

23.) Moreover, rippled does not require any validator to use any dUNL, or include any validator in particular in its own UNL.<sup>71</sup> Dr. [REDACTED] never explains why XRP Ledger nodes could or would not just switch to another already-published UNL.

56. Dr. [REDACTED] assumptions about the consequences of Ripple's disappearance also ignore that the XRP Ledger offers significant additional advantages to its users, such as increased speed and decreased transaction cost, with less negative environmental impact. (Adriaens Report at 22, 24–25.) These advantages – validating transactions in seconds, compared to approximately 10 minutes for Bitcoin – provide a significant value proposition for the XRP Ledger and an incentive for those who are interested in facilitating or enabling rapid decentralized settlement of transactions. (Adriaens Report at 22.)

57. While Dr. [REDACTED] report focuses narrowly on “in-protocol incentives” offered by Bitcoin and Ethereum (Report at 10 and 16), he ignores the significant competitive advantages that the XRP Ledger offers and the corresponding incentives for those interested in the success of such an ecosystem. (Adriaens Report at 25.) It is therefore unsurprising that participants in the XRP Ledger ecosystem – from exchanges like Bittrue to developers like XRPL Labs – operate validators without the need for in-protocol incentives.<sup>72</sup> Dr. [REDACTED] report offers no basis to conclude that these validator operators (whom I offer as mere examples of the over 120 validators currently active on the XRP Ledger system)<sup>73</sup> would cease operating their validators if Ripple were to disappear, and accordingly no basis to believe the XRP Ledger itself would disappear without Ripple.

---

<sup>71</sup> See *supra* note 64.

<sup>72</sup> See *Validator Registry*, XRPSCAN, <https://xrpscan.com/validators> (as observed Nov. 11, 2021).

<sup>73</sup> *Id.*

I declare under penalty of perjury that the foregoing is true and correct.

Executed on November 12, 2021

A handwritten signature in black ink, appearing to be 'PA', written over a horizontal line.

Peter Adriaens